Dense and randomized storage and coding of information

Abstract

We describe a method for dense encoding of information. Bennet and Wiesner (Phys. Rev. Lett. 69:2881-2884, 1992), using EPR-pairs, showed that n bits can be encoded by n/2 quantum-bits, from which the original bits can be retrieved. Here, in a completely different (non-quantum) setting, we give a method for more dense encoding: In our method n bits $x_1,x_2,....,x_n$ are mapped by a linear transform B over the 6-element ring Z_6 to numbers $z_1,z_2,....,z_t$ from ring Z_6 with $t=n^{o(1)}$(i.e., much fewer numbers) (Quantity o(1) here denotes a positive number which goes to 0 as n goes to infinity), then, by applying another linear transform C to these zi's, we will get back n elements of ring Z_6, $x'_1,x'_2,....,x'_n$, where, e.g., x'_1 may have the form $x'_1=x_1+3x_2+4x_3$. One can get back x_1 simply by running through the values of x_i on the set 0,1,2,3,4,5, and noticing that only x_1 has period 6, ($3x_2$ has period 2, $4x_3$ has period 3). Our results generalize for any non-prime-power composite number m instead of 6. We also apply this method for fast computation of matrix multiplication and for compacting and extending matrices with linear transforms.